```
NBG3KUNM
     UNITED STATES DISTRICT COURT
1
     SOUTHERN DISTRICT OF NEW YORK
     -----x
 2
 3
     KUNSTLER, et al.,
 4
                   Plaintiffs,
                                            New York, N.Y.
                                            22 Civ. 6913 (JGK)
5
                V.
6
     CENTRAL INTELLIGENCE AGENCY,
     et al.,
 7
                   Defendant.
8
        -----x
                                          Motion
9
                                            November 16, 2023
10
                                            2:30 p.m.
     Before:
11
12
                         HON. JOHN G. KOELTL,
13
                                            District Judge
14
15
                              APPEARANCES
16
17
     THE ROTH LAW FIRM, PLLC
          Attorneys for Plaintiffs
18
     BY: BRIAN S. LEVENSON
19
            RICHARD A. ROTH
            ROBERT BOYLE
20
     DAMIAN WILLIAMS
21
          United States Attorney for the
          Southern District of New York
     JEAN-DAVID BARNEA
22
          Assistant United States Attorney
23
24
25
```

THE DEPUTY CLERK: Will all parties please state who they are for the record.

MR. LEVENSON: Good afternoon, your Honor. This is
Brian Levenson from The Roth Law Firm for the plaintiffs. I'm
joined by Richard Roth of The Roth law Firm, and Robert Boyle,
of counsel to The Roth Law Firm.

MR. BARNEA: Good afternoon, your Honor. This is J.D. Barnea from the U.S. Attorney's Office for the federal defendants.

THE COURT: All right. This is a motion to dismiss so I'll listen to argument. Mr. Barnea.

MR. BARNEA: Should I do it from here, your Honor, or at the podium?

THE COURT: Whatever you wish. Whatever is more convenient.

MR. BARNEA: Thank you, your Honor. As a tall person, it is nice to have a little bit of a taller desk.

May it please the Court, your Honor, I would like to focus the federal defendants' presentation today on a few key arguments.

THE COURT: Before you do that, could I make sure that I understand some things at the outset.

There are claims against former Director Pompeo, as well as against the government. The claim or claims against Mr. Pompeo are solely for damages under *Bivens*, and the claim

against the defendant is for injunctive relief.

MR. LEVENSON: Yes, that's correct, your Honor.

THE COURT: Fine.

Second thing, at the outset, the government's arguments for dismissal against Mr. Pompeo are 12(b)(6) arguments. There is no *Bivens* claim. Even if there were a *Bivens* claim, there is qualified immunity. There is no standing argument with respect to Mr. Pompeo, and no other 12(b)(1) argument.

MR. BARNEA: That's correct, your Honor.

THE COURT: I ask that because I have to decide 12(b)(1) first. There is the standing argument against the claim against the government, so with that, at least having clarified things for me, go ahead.

MR. BARNEA: Thank you, your Honor.

So as I said, I'd like to focus the federal defendants' presentation today on a few key arguments, standing, as you just mentioned, the applicability of the Fourth Amendment to the searches and seizures at issue, the Fourth Amendment's reasonable expectation of privacy, and the plaintiffs' *Bivens* claim against Mr. Pompeo.

On standing, plaintiffs' claim seeking injunctive relief against the CIA cannot go forward because they allege no ongoing or imminent injury.

Plaintiffs claim that the CIA was involved in searches

and seizures that supposedly took place in 2017 and 2018 and that, to their knowledge, nothing has happened to the seized or recorded information in the intervening seven or eight years.

They do not allege that the CIA or anyone else has done anything with the information since that time or imminently plans to.

Even accepting plaintiffs' allegations as true, whatever information was seized from them could easily be sitting at the bottom of a file cabinet, entirely forgotten. That is not enough to allege an ongoing or imminent future injury as required by Article III. Even if the plaintiffs had standing to bring their claim, they cannot allege a Fourth Amendment violation.

THE COURT: By the way, they do allege an ongoing concern that the information that's been seized can be disseminated, and they want the return of the information now, right? What controlling cases do you think stand for the proposition that that's insufficient for standing?

MR. BARNEA: Well, again, the bedrock Article III requirement for standing for seeking injunctive relief, forward looking relief, is an ongoing or imminent injury.

Here, they hypothesize someone might do something with their information, but they don't have any reasonable claims of anyone imminently planning to do anything with that information.

THE COURT: My question really is what case or cases comparable do you rely on for that are proposition? That the government, having allegedly taken information, and still keeping that information with the possibility that the information can then be disseminated, and a party says you have my information, I want it back. Your continuing detention of the information is harmful.

What case or cases with that fact pattern do you think are most persuasive? I know the general rubrics of standing.

Trust me.

MR. BARNEA: Of course.

THE COURT: But what case or cases do you think are comparable?

MR. BARNEA: Well, I think the *Phillips* case from the Ninth Circuit is useful, in that their information was allegedly procured in violation of the Constitution and, granted, in different circumstances than what we're talking about here. And the court noted that in order for a plaintiff to seek expungement of that information, the plaintiff has to allege a potential future harm or imminent future harm that they expected the government to use this information in some way, so they could seek injunctive relief.

Again, it is clear that a person experiencing what they allege to be a Fourth Amendment violation is an injury, but it is a question as to whether it is ongoing or future

imminent injury, as opposed to simply a past injury.

There is no case that we have that's on directly on point to a one-time event that occurred many years with apparently nothing having happened in the interim.

The cases that plaintiffs rely on, for example, ACLU v. Clapper, is very much the opposite. The Second Circuit's decision there involved an ongoing program in which every day, the government was receiving telephone metadata including all -- all Americans' telephone metadata, including necessarily the plaintiffs, and was consistently querying that information was necessarily involved as the court found looking through the database in which the plaintiffs' data was contained. And so that, there, I don't think there is any question that there is an ongoing injury that the court could find standing for the plaintiffs to challenge.

But, I don't know how ACLU v. Clapper would have come out if the plaintiffs there had alleged a single incident of information being taken years ago, yet they are seeking forward looking injunctive relief.

THE COURT: $ACLU\ v.\ Clapper$ talked about not only the collection of the information, but the maintenance in the government's database.

MR. BARNEA: Right, and again, maintenance there I think is different from what we are talking about the allegations in this case. In that case, the maintenance was an

actively used and regularly accessed database that was, as described in the Second Circuit's opinion, one that the government regularly looked at and necessarily, by consistently examining that database, was sort of necessarily looking through, among other many other records, the plaintiffs' own records.

So it wasn't simply that it existed at the bottom of a file cabinet somewhere. It was that it was maintained and in active use by the government over time.

THE COURT: Okay. Go ahead.

MR. BARNEA: Even if the plaintiffs had standing to bring their claim, they cannot allege a Fourth Amendment violation, because the Fourth Amendment is not applicable to the alleged conduct at issue. In order for the Fourth Amendment to apply to the conduct of foreign persons, the U.S. government must play a sufficient role in controlling or directing those foreign persons' actions.

Here, plaintiffs have not alleged sufficient facts that, if proven, would establish that the CIA controlled or directed the Spanish defendants. Plaintiffs assert that the Spanish defendants were approached by intermediaries, supposedly on behalf of the CIA, to conduct surveillance on Assange and his visitors. They claim that the CIA provided some technical assistance in implementing that surveillance, and they claim that the CIA promised contracts or remuneration

in exchange for the provision of that information.

None of those allegations, even assuming their truth, establish that the CIA controlled or directed the actions of the Spanish defendants.

The Second Circuit has already has articulated and applied the relevant standard in several cases involving U.S. government requests for information from foreign police forces and never found it to be satisfied. Those cases include the Lee, Getto, and Gasperini cases.

The fact that the U.S. government requested information from a foreign police force is not sufficient to implicate control or direction by the U.S. government, nor is it enough if a foreign police shares the results of the search with the United States government, including through a live video feed. The court has further concluded that the U.S. government's provision of money, equipment, and training —

THE COURT: The contemporaneous monitoring was done from the United States, wasn't it?

MR. BARNEA: In which case? In the *Getto* case?

THE COURT: No, no, in this case allegedly.

MR. BARNEA: I don't think they specified the location, but I imagine that is what they're claiming. I believe that would be the same also in the *Getto* case.

THE COURT: So, U.S. agents were monitoring the feed in the United States, and that's not sufficient involvement by

the government?

MR. BARNEA: The question is not -- the relevant test is not involvement by the government, but control and direction over the foreign actor by the U.S. government.

So, the question is were the people who were doing the actual searches and seizures abroad controlled and directed by the U.S. government in the relevant sense in order to implicate the Fourth Amendment. And I was simply going over the various ways that the court has found do not satisfy that standard, including the U.S. government's provision of money, equipment, and training to the foreign police force, which also does not implicate the U.S. government in their actions, as well as the fact that the search by the foreign government was at the request of the U.S. government or that the results of the search or a live feed of whatever it was, was provided to the U.S. government.

THE COURT: Why isn't there at least an issue of fact as to what the involvement of the government was?

MR. BARNEA: Well, this is not a question of fact. We are saying that if you look at the allegations in the plaintiffs' complaint of the CIA's involvement here, it does not rise to the level that would satisfy the standard. So we're not questioning for this purpose what those allegations are or the truthfulness of the allegations. The question is have they alleged a sufficient role for the CIA that would

demonstrate that the CIA, assuming those allegations were ultimately proven true, controlled and directed the actions of, here, the Spanish defendants.

And in our view, as a matter of law, those allegations are insufficient, because they have not established that the CIA controlled and directed. They have established that the CIA may have asked for information and may have provided technological assistance and may have offered something in return if the information was provided. But in our view, that simply is not control and direction.

THE COURT: Why isn't it at least direction? Is it sufficient for direction without control?

MR. BARNEA: Well, the Second Circuit uses the sort of combined phrase "control and direction," and I have to say that given that the Second Circuit has never found this standard to be satisfied, nor have I found any District Court cases that have found it to be satisfied, it is hard to identify exactly what circumstances would satisfy the standard.

We can all hypothesize when, if someone was literally essentially working as a contractor for a federal agency or something like that, you might conclude it was satisfied. But it's hard to say exactly how the Second Circuit or when the Second Circuit would find the standard to be satisfied, given that we have never seen a case where it was.

THE COURT: Okay.

MR. BARNEA: Even if the Fourth Amendment applied, plaintiffs cannot claim a Fourth Amendment violation with respect to plaintiffs' alleged conversations with Assange at the embassy, their passports and the exteriors of their electronic devices, because they did not have a reasonable expectation of privacy.

The Fourth Amendment's protections only apply when a person reasonably believes that their conversations are private from others, or that no one else has access to the items at issue.

As explained in our briefs, courts have repeatedly held that, because government buildings and the like so commonly have security cameras and other surveillance equipment in them, both visible and invisible to visitors, there is no reasonable expectation of privacy in such a facility, unless the person is given explicit assurances of privacy.

Thus, for example, in a police station, courts have held there is no reasonable expectation of privacy in any part of the building, even when there are no other people around, and when there are no visible cameras or microphones, except when the person is told that a particular place is private. Like the rooms where arrestees are told they can meet with their lawyers confidentially.

Similarly, plaintiffs concede it is reasonable to assume there is some surveillance cameras and the like in a

foreign embassy. That defeats their claim since they do not allege that anyone at the embassy told them they would be able to have private unmonitored conversations with Assange.

Plaintiffs' argument they didn't know their information would be shared with the CIA specifically is a red herring. The relevant question is not whether plaintiff had a reasonable expectation that their information would not be shared with the U.S. government. Rather, it is whether they had a reasonable expectation that their communication was private, and that no other people could have been listening to it, regardless of who those other people might have been or the purpose for which they might have been listening.

This is why no one has a reasonable expectation of privacy in a conversation taking place in Penn Station, even if they didn't know that an undercover officer was eavesdropping on them.

As for their passports and the exteriors of their electronic devices, the law is clear that simply turning them over to the embassy's security desk eliminates their expectation of privacy in those items. This is so regardless of whether they knew or had reason to believe that the security desk might further share these items with anyone else.

As a related point, even if they had a reasonable expectation of privacy, plaintiffs' communications with Assange would not violate the Fourth Amendment, because any

surveillance of such communications would have been reasonable
As the Second and Ninth Circuits have explained, the Fourth
Amendment doesn't apply at all to searches of foreign citizens
outside the United States. And as long as the search as
long as the search of such a foreigner abroad is generally
reasonable, then it does not violate the Fourth Amendment for
the U.S. government to capture the foreigner's communications
with U.S. persons. No warrant or other approval is needed for
the U.S. government to monitor a foreign person's
communications, even when those communications are with U.S.
persons. As long as the U.S. government is legitimately
monitoring the foreign person's communications, and not using
that as a pretext to monitor the U.S. person's communications,
this does not violate the Fourth Amendment.

Here, Assange was a foreign citizen located outside the United States, so the Fourth Amendment doesn't apply to any surveillance of him. He was also being investigated at the time for various criminal acts, so any surveillance of him would have been reasonable. It follows that if such surveillance captured his communications with U.S. persons, that would not run afoul of the Fourth Amendment.

As for plaintiffs' Bivens --

THE COURT: But you take us up to the point where the plaintiffs allege that the contents of their electronic devices were seized. And you don't seem to dispute in your papers that

a warrant would be necessary to seize the contents of the electronic devices.

MR. BARNEA: I don't believe that a warrant is ever required outside the United States. The Second Circuit has held that the warrant requirement of the Fourth Amendment only applies within the United States.

THE COURT: What case is that?

MR. BARNEA: The Bombing in East Africa —— I'm sorry.

U.S. Embassy Bombings in East Africa, among others, have held

that the warrant requirement specifically of the Fourth

Amendment does not apply extraterritorially. There is

nonetheless a reasonable requirement that applies from the

Fourth Amendment to surveillance by the U.S. government of U.S.

persons abroad.

THE COURT: No, no, no. We're talking about the plaintiffs' allegation that their electronic — they left their electronic devices as well as passports, and that the outside were copied. And you said no expectation of privacy with respect to that.

And then there is the section that deals with the fact that the plaintiffs allege that the contents were copied. And the only response that I saw in your papers was not no warrant is required outside the United States. You assume that a warrant is required for the contents of Americans' electronic devices that are left at the embassy abroad. But you say the

plaintiffs haven't alleged that no warrant was obtained.

MR. BARNEA: That's not precisely what we argued, but if I am allowed to clarify.

THE COURT: Sure.

MR. BARNEA: This may be of limited importance given what I am going to say. But, I don't think that we ever conceded that -- I mean, to be clear, the warrant requirement of the Fourth Amendment does not apply abroad. I think our argument on this point was that when the plaintiffs say that the search was illegal, that is simply a conclusory statement. They have not alleged in what way it is illegal. And we gave examples of domestic cases where there were more specific allegations of whether a warrant was required or a warrant was obtained improperly.

In any event we actually, we rereviewed the plaintiffs' opposition brief, and in a footnote they mentioned a potential amendment that they might seek to make of their complaint in this regard, which we had missed before, because it was sort of buried in a footnote. But if they had made that kind of an allegation, I'm not sure we would have made a similar argument having to do with what they viewed as the lack of need for a warrant or the unreasonableness of the search, and so that potentially could cure that particular objection, that particular aspect of our motion.

THE COURT: I frankly don't understand what you just

said.

MR. BARNEA: Okay. I'm happy to answer any questions about it.

THE COURT: So let's take it from the top so to speak.

I had thought your brief did not dispute that a warrant is required for the contents of electronic communications. And certainly there is case law in the United States that stands for that proposition. You need a warrant in order for the government to seize the contents of a phone.

MR. BARNEA: Right. In the United States, the government needs a warrant to seize the contents of a phone.

THE COURT: And I read your papers as saying the plaintiffs haven't alleged in their papers that no warrant was obtained in this case. And therefore, they have failed to state a claim for a violation of the Fourth Amendment. And that's the way in which I read your papers.

You're telling me, no, that's not what you said. I'll go back and read your papers with much more care. They were read with care initially.

MR. BARNEA: No doubt, your Honor.

THE COURT: That of course raises the next question, which is the government should know whether a warrant was obtained or not. What you're telling me now is, I think, the implication of what you're telling me is of course there was no warrant. No warrants are required to seize the contents of a

2

3

4

5

6

7

8

9

10

11

12

13

14

15

16

17

18

19

20

21

22

23

24

25

	phone	from	an	American	citizen	abroad.
- 1		_	_			

MR. BARNEA: So, allow me to try to clarify my statement, and I apologize if I wasn't clear earlier.

The constitutional warrant requirement of the Fourth

Amendment does not apply outside the United States. So, as a

result of the Constitution, no warrants are required for any

searches that occur outside the territory of the United States.

There are certain statutory provisions that may --

THE COURT: Okay. Let's pause there. And you rely on East Asia Bombings?

MR. BARNEA: East Africa Embassy Bombings sets out relatively clearly. I think other cases, Hasbajrami.

THE COURT: Did you cite East Africa Bombings?

MR. BARNEA: It is cited in one of our briefs.

THE COURT: No, in your initial brief.

MR. BARNEA: I'm trying to remember what brief we cited it in.

THE COURT: It doesn't appear in your table of --

MR. BARNEA: It's in re -- let me find it.

THE COURT: If it's In re East Africa Bombings, it's not in your initial brief.

MR. BARNEA: It might be in the reply brief then.

THE COURT: Okay.

MR. BARNEA: In re Terrorist Bombings of U.S. Embassy in East Africa cited on page 8 of our reply brief.

THE COURT: So, you say no warrant was required.

MR. BARNEA: Here it is on page 8 of our reply brief. This is a Second Circuit case from 2008, holding that the Fourth Amendment's warrant clause has no territorial application and that foreign searches of U.S. citizens conducted by U.S. agents are subject only to the Fourth Amendment's requirement of reasonableness.

THE COURT: So, in your initial brief you argued, I thought, again, I'll go over it, that the plaintiffs failed to argue that there was no warrant for the seizure of the contents of the cell phones.

Did I misread that argument?

MR. BARNEA: We argued that they simply posited that the search was illegal, but did not specify in what way it was illegal, such as, for example, if they thought a warrant was required, to explain what warrant might have been required, and why it wasn't obtained or how it was obtained improperly.

So the perhaps that's why our brief was confusing for your Honor, and I apologize for saying that.

THE COURT: That certainly does suggest that the problem with their complaint was the failure to allege that a warrant was obtained. So, but your argument is no warrant was required.

MR. BARNEA: No warrant was required by the Constitution.

THE COURT: So, can I take it from your argument that the government concedes that there was no warrant that was obtained, because no warrant was required?

MR. BARNEA: Again, certain statutes may require warrants in certain circumstances, even if the Constitution doesn't mandate it.

We neither concede nor have any statement about whether any warrant was needed or was obtained in this case, because of course none of the facts of this case we are having any factual comment on them.

I think our point was meant to be, and again, this is not a point that we think we need to pursue much given the statement that we saw about a potential amended allegation that the plaintiffs might make in this regard.

But our point was simply that by claiming that the search was illegal without explaining why it was illegal, the plaintiffs had not -- were making a conclusory statement without actually justifying the pleading that they were trying to make.

THE COURT: Here's my problem with that argument. The government knows whether a warrant was obtained or not obtained. If the government knows that there was no warrant, then I wonder whether in good faith the government can make the argument that ah-ha you haven't alleged that no warrant was obtained, when the government knows as a matter of fact that no

warrant was obtained.

MR. BARNEA: Again, we're not here to -- I'm not at liberty to comment about whether a warrant was required or was obtained, whether it was required by statute or by the Constitution or something else.

THE COURT: But, here's --

MR. BARNEA: Again, we never --

THE COURT: Hold on.

MR. BARNEA: Sorry.

THE COURT: Here's my problem with making that argument, just to be clear. It's not clear to me whether the government can argue in good faith, without any explanation, with respect to some of the defenses that the government sometimes raises, that it is a matter of national security simply to say we cannot affirm or deny whether there was a CIA offices in that particular country.

When the government tells me in this case that simply that they haven't alleged that there was no warrant, when the government knows full well whether there was a warrant or not, seems to me stretching the bounds of good faith. I mean, it doesn't seem that that's an argument that the government could make when the government knows full well that hypothetically there was no warrant because it's not required under the Constitution. Putting aside for a moment whether it was required under any statute. Do you follow at least my --

MR. BARNEA: I understand. And again, this is not an argument that we're pressing in light of a -- or that we think that this argument may well be solved by a statement in their opposition brief that we initially overlooked, so this is not an argument that we're pursuing. But in --

THE COURT: What's the statement that you overlooked and that I may have overlooked also?

MR. BARNEA: Page 14, footnote 10 of the opposition brief.

THE COURT: One of my favorite footnotes.

MR. BARNEA: Which has to do first with about whether or not we had raised certain issues in our premotion letter, and later on in the same footnote, they proposed how they might have amended their complaint to deal with this particular argument, and they assert that this argument could have easily been corrected in the first amended complaint as there was no search warrant in existence -- I'm sorry.

THE COURT: I see it.

MR. BARNEA: That the plaintiffs were aware of no basis for obtaining a search warrant for plaintiffs.

Again, without a statement -- it is a little complicated, but in any event, our argument was not based on specifically whether a search warrant specifically was available, but rather whether there was any basis to the allegation of the search being illegal. Our objection was

simply to the legal conclusion of the search having been illegal, without any explanation as to why they concluded that the search was illegal.

THE COURT: So, assume that the plaintiffs now say that there was no search warrant. And the response is? Hasn't been briefed.

MR. BARNEA: Well, again, if they said something along the lines of we are not aware of any search warrant, and in any event, the search that was conducted was not reasonable, and in our view, that would cure the pleading defect that we identified and would allow that particular claim to survive. Assuming that the Fourth Amendment applied and they had standing to bring it, which of course there are objections to that particular claim.

THE COURT: All the plaintiff has to do to make this claim survive is to allege that there was no search warrant, and a search warrant was required to make the search reasonable.

MR. BARNEA: Well --

THE COURT: You say if the plaintiff had only said that, this claim proceeds.

MR. BARNEA: No. I said if they had standing, and if the Fourth Amendment applied at all, which in our view it does not, because the search at issue was conducted by a foreign actor who was not controlled and directed by the CIA.

But if the plaintiff can overcome those two issues, and the only issue was whether they had adequately pleaded a Fourth Amendment violation with regard to someone taking their cell phones, then, in our view, an allegation that they are not aware of any search warrant being obtained, they are not aware of -- and in their view, the search was unreasonable, either because of an absence of a search warrant or for other circumstances, that may well cure the particular pleading sufficiency that we identified in our brief. We would have to study precisely what they would allege in that regard. This is why we think it would be relatively easy to overcome that particular argument, which is why I wasn't planning to focus on it today.

THE COURT: I'm sorry, you think it would be relatively easy to overcome that argument?

MR. BARNEA: We think that if they made that type of an allegation, it would resolve that particular aspect of our motion to dismiss, in all likelihood. Which is why we are not focusing on that aspect of our motion to dismiss.

THE COURT: Well, there is a fully briefed motion. It includes an argument that the plaintiffs have no claim with respect to the seizure of the contents of their electronic devices abroad. And you argued that that claim falls in part because they haven't alleged the absence of a warrant.

MR. BARNEA: No. All they had alleged, all they

allege in their complaint is that someone took their phone and it was, quote, illegal. That was all they alleged.

So, what we point out was, by simply labeling something illegal, that is a conclusory statement. They haven't explained why it is illegal. And now, in this footnote they have demonstrated what it is they might argue or how they might plead more specifically why it was illegal, and I was trying to explain to the Court why, in our view, if they were to amend their complaint along these lines, that may well resolve the concern that we had raised.

It was simply about the conclusory nature of the label "illegal" being applied to something, without any explanation as to what about the search was illegal or why it was illegal.

THE COURT: Okay. I'll revisit this of course with the plaintiffs in a moment, but it would seem to me unnecessarily wasteful to tell the plaintiffs file a motion to dismiss, denied, or granted, with leave for the plaintiff to file an amended complaint which includes more specific allegations with respect to the seizure of the contents of the electronic devices.

I mean, there is a fully briefed motion that should be decided, and for the reasons that I've suggested, I didn't find the briefing very clear on that.

MR. BARNEA: Apologies, your Honor.

THE COURT: No, no, never apologize. It would seem to

me that plaintiffs could simply file an amendment to the complaint with respect to their specific claims with respect to the seizure of the contents of the electronic devices. And the government would have the opportunity to file a motion directed to that amendment, and the plaintiffs could respond, the government could reply, rather than repleading the entire motion.

MR. BARNEA: Your Honor, we don't think that the Court is even going to have to reach those issues necessarily, given our fundamental standing and inapplicability of the Fourth Amendment. But if the Court wishes for us to examine a proposed new pleading, we're happy to do so. And as I've already said, it seems likely that they would be able to satisfy us in this regard. So, this may be not much of an exercise at all.

THE COURT: Okay. Go ahead. You may have just been about concluded.

MR. BARNEA: Yes, well, I was just getting to the Bivens point. Let me find my notes.

THE COURT: I fully appreciate that this is a new area for *Bivens*, that it's never been applied in the context of national security and abroad. And that there are reasons to believe that Congress wouldn't believe that a *Bivens* remedy would be appropriate under the circumstances of this case, given the administrative remedies that are available.

MR. BARNEA: Precisely. That is exactly our argument.
That this is not an area in which any Court could reasonably
conclude that Congress wanted the judiciary to create a remedy,
as opposed to limiting itself to the remedies Congress itself
has created, which include this very lawsuit against the CIA,
options to complain to the CIA's Office of Inspector General
and the like, which are very similar to the types of alternate
remedies that the Supreme Court has recognized as sufficient
alternate remedies in other proposed Bivens cases, and rejected
the Bivens remedy.
So, seems like our argument is relatively

So, seems like our argument is relatively straightforward in that regard. So, those are the only points I wanted to make. I'm happy to answer any further questions that your Honor might have about our arguments.

THE COURT: No. You weren't going to touch on qualified immunity? I know the argument of qualified immunity.

MR. BARNEA: I am happy to summarize it for the Court.

THE COURT: No.

MR. BARNEA: I had selected a few of our arguments I wanted to highlight in the argument today.

THE COURT: I'm familiar with the qualified immunity argument.

MR. BARNEA: And at bottom, we are talking about whether there is sufficient allegations of Mr. Pompeo's personal involvement in the alleged acts, and we simply think

an examination of the complaint, putting aside conclusory statements of Mr. Pompeo approving things or directing things which have been held in other cases to not be sufficient, are simply not sufficient to implicate him personally. So therefore, even if there were a *Bivens* remedy, he would be entitled to qualified immunity for lack of personal participation.

THE COURT: Okay. Thank you.

MR. BARNEA: Thank you, your Honor.

THE COURT: Plaintiffs.

MR. LEVENSON: Good afternoon, your Honor. This is Brian Levenson for the plaintiffs.

There is no doubt that the plaintiffs have standing to pursue this case under settled Second Circuit law, notably the ACLU v. Clapper. The Second Circuit has held that the collection, maintenance, and retention of seized information in a government database is sufficient for standing to pursue a claim. Whether or not that claim ultimately prevails is different than whether or not the plaintiffs have standing to pursue it.

The government relies on *Phillips*, which is a Ninth Circuit case and not binding on this Court. Further, *Phillips* is easily distinguishable on many grounds, including the plaintiffs in that case were migrants as part of a caravan coming to the United States who do not enjoy Fourth Amendment

rights, the information in the government database was independently created by the government, it was not seized from any of the plaintiffs in that case, and the plaintiffs migrants wanted the destruction of that information that was independently collected and gathered by the government.

This case has no resemblance, even if it was controlling. These are U.S. citizens, protected by the Fourth Amendment, even abroad. And the government, without a warrant, though it may not have been specifically pled in the complaint, it was pled without authorization, unconstitutionally and illegally, seized not only the content of their electronic devices, laptops, cell phones, but also recorded private conversations between the plaintiffs and Julian Assange, the plaintiffs being lawyers and journalists.

There is case law, including cases cited by the government, that there is a higher expectation of privacy with respect to attorney-client communications. The plaintiffs had no idea that their cell phones and laptops would be searched at an embassy in London.

And further, the government has raised the argument that they should assume there is some level of lack of privacy. But that's not what's required. Absolute privacy, absolute solitude is not the standard. It is reasonable. Was it reasonable. They would not have brought electronic devices carrying every bit of their lives with them or engaged in those

conversations in that room had there been any expectation that the CIA was listening.

THE COURT: Could we divide all of that up.

MR. LEVENSON: Okay.

THE COURT: There are arguments with respect to what you can expect reasonably with respect to surveillance at an embassy abroad. But, you've mixed up, if you will, in the same sentence, the surveillance that occurred abroad, and the search of the contents of their electronic devices that include lots of things that went beyond simply the surveillance at the embassy.

And the government initially said you didn't specify how that search of the electronic devices was unreasonable or without a warrant. And when you go back and forth from the footnotes and listening to the government today, if you made a few more allegations with respect to the seizure of the contents of the electronic devices, the government has indicated that, at least as I understood it, that part of the specific argument that related to the seizure of the contents of the electronic devices would fall out.

What I was trying to say to the government was, there should be a simple way for the plaintiff to add some additional allegations to the complaint to which the government might not have the same additional argument that it had raised to the seizure of the contents of the electronic devices, and we can

move on without having a whole new briefing of the entire motion.

I mean, I can accept a letter which, you know, amends the allegations in the complaint, and a government response as to what the argument, if any, is with respect to that amended allegation, and decide the entire motion without having leave to file an amended complaint, deny the initial motion as moot because there is an amended complaint.

Doesn't that make sense to you?

MR. LEVENSON: Yes, it does, your Honor. That's what we proposed in footnote 10, to the extent this was really an issue.

THE COURT: Okay. So, what do you propose specifically?

MR. LEVENSON: Yes, a letter amendment. We could just -- without amending the entire complaint, we can amend a specific paragraph or just include additional allegations sufficient to show that the search and seizure was unreasonable and without a warrant to satisfy the government.

THE COURT: The search and seizure of the contents of the electronic devices.

MR. LEVENSON: Yes, your Honor.

THE COURT: And you would file that letter amendment soon?

MR. LEVENSON: Within a week, your Honor.

Thanksgiving eve.

THE COURT: Next week is Thanksgiving. So you can take two weeks.

MR. LEVENSON: Thank you, your Honor.

THE COURT: And the government can file its response December 8th.

MR. BARNEA: Thank you, your Honor.

THE COURT: And if there is any reply, December 13. Okay?

MR. LEVENSON: Yes, your Honor. Thank you.

THE COURT: Great. So, go ahead.

MR. LEVENSON: So that tables the standing issue for now as I take it.

With respect to the government's issues with a lack of specificity in allegations of direct and control, the complaint provides every piece of information about the government's direction and control, including who, what, where, when, how, and why.

It occurred at the SHOT convention in Las Vegas, between the Las Vegas Assange security team at the direction of the CIA recruiting U.C. Global and Morales, who already had the contract for private security at the Ecuadorian embassy in London. And the purpose was, we allege, a personal vendetta between the director of the CIA, Mike Pompeo, against Julian Assange.

Mr. Pompeo in his first speech said that was his top priority, that was what he addressed, is Mr. Assange was a non-state hostile foreign actor, and WikiLeaks the same, and he wanted to crush them more or less.

He goes on in his memoir containing additional allegations against Mr. Assange that is not in the complaint, that was published after, but that is the why, and the how is the most specific thing. That the CIA provided software, written in English, to U.C. Global, the security company who had the embassy contract, about how to install real live time feed surveillance of Mr. Assange at the direction, approval, and authorization of Mike Pompeo.

It is unclear what more the plaintiffs could have alleged when we don't know the ins and outs of the secret clandestine attempt to surveil not only Mr. Assange, but anyone who comes in contact with him, whether it is a journalist, a lawyer, a doctor, who the complaint alleges were the targets of this. And it was not a one-time thing. It was ongoing. The complaint identifies over 100 Americans visited Mr. Assange at the embassy, including actress Pamela Anderson who it later came out that video of Ms. Pamela Anderson with Julian Assange in this conference room was on David Morales's laptop in a folder marked CIA.

Again, that information was published after the complaint, but it's included in our briefing, because it

certainly connects the plausibility that Mr. Pompeo and the CIA were at the direction and control — were directing and controlling the security team at the embassy, U.C. Global, that they reported, and they were in fact, they're on payroll. This was paid for.

The government made the argument, oh, there is no problem if foreign governments want to share information. This was not a foreign government. This was a private security contract. These are not government actors. These are regular people who have a security contract at a London embassy. This is not information sharing among nations. This is private actors on the payroll, bought and paid for by the CIA. Recruited by Mike Pompeo and under his supervision. The CIA directed and controlled this operation.

The clincher, the plausible, undeniable, is also in our brief at the very end, through reporting that came out again after the complaint, was that the U.S. government within hours disrupted a conversation between Mr. Assange and the Ecuadorian government that would provide him diplomatic status, within hours it was disrupted. That could only be done with real live time feed of that room and what was being discussed, and it certainly makes clear it is not information sharing between foreign government. This is was the Ecuadorian government that was being spied on. And this was done by private actors, David Morales and U.C. Global.

So again, this is not a request for information from a foreign government; it is not sharing by a foreign government.

With respect to reasonable expectation of privacy, I started to address this, and your Honor was correct that I should break it out. But Riley v. California, the U.S. Supreme Court case from 2014, makes clear in fact the "With respect to cell phones, get a warrant."

THE COURT: Right. That's with respect to the contents of the cell phone.

MR. LEVENSON: Yes. That is the allegation in the complaint.

THE COURT: No, no question. The complaint alleges that the content of the electronic devices were in fact seized.

MR. LEVENSON: Yes.

THE COURT: And that a warrant is required under Riley. There is the separate argument, because you also say there was a Fourth Amendment violation because the materials that the plaintiffs left at the desk, including their passports, were also copied, and that that was a violation of the Fourth Amendment.

MR. LEVENSON: The inclusion of the allegation regarding passports was not an allegation of violating the Fourth Amendment. That was an allegation to show that the CIA was on notice these were American citizens.

THE COURT: Oh.

MR. LEVENSON: At the time that they entered the embassy.

THE COURT: So there is no allegation that the copying of the materials that were left when the plaintiffs entered the embassy was a violation of the Fourth Amendment.

MR. LEVENSON: Not the passport, your Honor. I want to distinguish it from the electronic devices. It is a totally separate issue, which that is a violation of the Fourth

THE COURT: The contents of the electronic devices.

MR. LEVENSON: Yes.

THE COURT: Not the outside of the electronic devices.

MR. LEVENSON: We are not alleging a Fourth Amendment violation based on taking a picture of the outside of a passport or a phone or a laptop.

THE COURT: Okay.

MR. LEVENSON: That is a tremendous fact in this case that the search, that the seizure, were separated in time and space, where they checked — just as I came into the building today and had to check my phone, the government knows who I am, if I provided my passport, they know that I am an American citizen, they have my phone, and *Riley* makes that off limits. That's off limits.

THE COURT: I know that's the content of the phone. I got it.

MR. LEVENSON: I don't want to belabor the point, yes.

THE COURT: You also argue, I think, that the surveillance of the meetings with Assange was also a Fourth Amendment violation.

MR. LEVENSON: Yes, that's what I was going to. That is a Fourth Amendment violation, because at the moment where the plaintiffs checked into the embassy and checked their devices, and provided their passport, the government in real time knew these were American citizens about to enter the room, the room is separated, they went in the room, and now they're surveilling U.S. citizens without a warrant or without any reason. There is no reasonableness. These are not criminals, these are lawyers, doctors, physicians, journalists.

THE COURT: Is there any comparable case that says there is a Fourth Amendment expectation of reasonable expectation of privacy in a foreign embassy for an American citizen who has a conversation in a foreign embassy? Any sort of comparable case?

MR. LEVENSON: Your Honor, there is no case like this. I'm not even going to analogize any other case. There are many prison cases cited by the government, and we are just dumbfounded by the comparison. This is not a prison. He is a free person. Prisoners have no liberties, and of course there is no reasonable expectation of privacy in a prison. These are lawyers going to see a client at an embassy.

THE COURT: The argument can certainly be made that when people go into a foreign embassy, they would expect that there is security in the embassy that would cover surveillance in the same way that when you enter a courthouse, you can expect there is surveillance.

MR. LEVENSON: Yes, of courses there is surveillance, of course there are video cameras to keep track of who is in the elevator and the hallway and in case something happens. Of course, many buildings have surveillance. Any building would have surveillance.

But this is different. This is a private meeting in a separate room. These are not the public areas of that building. These are not common areas. These are private areas. And they're there to see a client or a source for an article. There is a reasonable expectation that under these circumstances, where they've identified themselves as Americans from the get-go, that they are not going to be surveilled by the CIA.

THE COURT: Why?

MR. LEVENSON: Because they've identified themselves as American citizens.

THE COURT: So?

MR. LEVENSON: The government is relying -- telephone wiretap cases involving terrorists. This is not a terrorist. This is not someone who called terrorists and was accidently

picked up and, oh my God, that is an American citizen, what do we do? It's okay, it is incidental overhear doctrine.

That's not what this is. It is separated. I am an American citizen, I am going in that room to talk to that person, I have a reasonable expectation that the government is not listening.

THE COURT: There is no allegation in the complaint that when the plaintiffs go into the foreign embassy they say, we want a private room in order to be able to talk to this person. These are going to be confidential discussions, we don't want anyone listening. Got it?

Would a foreign embassy be expected to say, oh sure. come on in, we'll give you a safe room.

MR. LEVENSON: No, that's not a reasonable conversation. The extent of -- let me find the case. *Mankani*, Second Circuit, 1984, the Fourth Amendment protects conversations that cannot be heard except by means of artificial enhancement, which is what this is. Tiny microphones bugged on fire extinguishers, special devices put on windows to obscure outside noises. That is the only way these conversations could be heard. And that is what the Fourth Amendment protects.

THE COURT: I assume *Mankani* is not in the context of a foreign embassy abroad.

MR. LEVENSON: No. We were unable to find any case

involving any foreign embassy. Any embassy.

THE COURT: Okay.

MR. LEVENSON: To be candid.

One thing I wanted to go back just to clarify about plaintiffs' allegations concerning the copying of materials. There is an allegation that the government dismantled a cell phone and took a picture of something called an IMEI card on the inside of the phone that permits the government extraordinary amounts of information with that code. We do allege that that's part of our claim for a Fourth Amendment violation. That is on the inside of the phone, not the outside.

THE COURT: Okay.

MR. LEVENSON: Finally --

THE COURT: The main argument with respect to the individual liability.

MR. LEVENSON: Yes, Bivens, yes.

THE COURT: Right.

MR. LEVENSON: Yes, your Honor. We believe that this is a *Bivens* claim. While *Bivens* was a search of a person in their own home who is handcuffed and was permitted to sue for damages, we believe this is worse. This is not just a search of a home. This a search of a phone. A phone has extraordinary amounts of information not available in a home. I don't need to tell you, your Honor, what could be on a phone.

GPS tracking location, health, medical records, client documents, client information, journalistic sources, personal pictures — compromising pictures, in fact — e-mails, personal text messages. This is so far beyond the search of a phone. Riley v. California made it clear that the phone is not — is off limits in this context. That was in 2014. These searches occurred after. It was no doubt what the law was at the time that these searches happened. Bivens was a Fourth Amendment case as is this.

whether there was a Fourth Amendment violation, and whether perhaps there was qualified immunity after *Riley*, rather than to the analysis of *Bivens*, which is whether the application of the Fourth Amendment to a new circumstance that has not been recognized by the Supreme Court. This is a long way away from *Bivens* itself. And there are only three cases where the Supreme Court has said, yes, that's a *Bivens* claim. We'll recognize it. And the kinds of distinction that the Supreme Court has drawn with respect to whether *Bivens* should be extended to a new situation would seem to argue that it shouldn't be extended here.

Your turn.

MR. LEVENSON: Sure. It's true there are only three instances, three cases where the Court applies *Bivens*. That is a case-by-case analysis. As I tried to argue, this is worse.

This is so much worse. *Bivens* is a man in his home. Whatever is in his home, is in his home. A phone has the data, sensitive data, sensitive messages that may not be kept in a home. It's a different circumstance only that rather than occur in a home, it occurred in an embassy.

We fail to see how that's the line to be drawn as far as whether this is a different context. It is the conduct that is the same. It is an unreasonable extreme action taken by the government at the direction of Mike Pompeo, and he is not entitled to qualified immunity because *Riley v. California* made it clear.

THE COURT: Separate argument from Bivens. Qualified immunity, separate argument from Bivens.

MR. LEVENSON: Okay.

THE COURT: National security, broad.

MR. LEVENSON: There is no national security implications with Ms. Hrbek or Ms. Kunstler. These are U.S. citizens who are lawyers, who had long distinguished careers representing clients either in entertainment transactions, litigations, sometimes civil rights cases, journalists. These are not terrorists. These are not terrorists. There is no immediate harm to the country. These are not people crashing the border. These are people going to see a client or journalistic source in a room, with a reasonable expectation of privacy. That's all this is. They are not terrorists, they're

not on any watch lists, they are not on a no fly list. They are just people, your Honor.

THE COURT: No one has suggested that they are. The national security interests are from Mr. Assange, whether those are correct or not, they are asserted. Right?

MR. LEVENSON: He is not the plaintiff in this case, your Honor. His phone was not downloaded and searched. He was not going to visit someone and have his conversations — and that's what I was getting at earlier. To the extent, putting Mr. Assange aside, which you can, because at the moment they walked in the door, they had done nothing other than they announced their intent to visit him. Fellow journalist, a client. And that is it.

THE COURT: Okay.

MR. LEVENSON: Thank you, your Honor.

THE COURT: Thank you.

Anything further?

MR. BARNEA: Thank you. I wanted to say a couple more things about whether the plaintiffs had a reasonable expectation of privacy in a foreign embassy.

Of course we also haven't been able to find any cases specifically taking place in foreign embassies, since I guess nobody has filed such a case that's been published on Westlaw so far. However, there are plenty of cases, and we cite a lot of them in our brief, that talk about different kinds of

circumstances in which someone does not have a reasonable expectation of privacy and why. And I wanted to just go over briefly some of those.

It is right that a couple of them have to do with jails, but I think a better analogy is police stations. So, for example, there's a case involving the front desk of a police station in which you have a circumstance where, when no one else was present, two police officers had a conversation, and they claim that the police department they worked for placed a secret microphone under the desk and was recording their conversations, and they sued. And the Court concluded that they had no reasonable expectation of privacy because they were in a police building, and it is an area that is open to the public, and people come by, and it is not reasonable for them to have an expectation of privacy in those circumstances.

Another case where the defendant was the Port
Authority was people were in a medical facility, no one else
was in the office with them, in the nurse office with them, the
nurse was not there. They thought they were having a private
conversation. They did not know there was a secret camera
installed in the room. And the Court held that they did not
have a reasonable expectation of privacy, because they were in
a medical facility, and people were going in and out of the
room, and people — and this is not the type of a location
where people can expect to have privacy. Even though, as far

as the people themselves were concerned, they were by themselves, and they didn't see any surveillance equipment.

So the question is not did someone know that they were being surveilled. The question is are you in a place where you have sufficient assurances of privacy, either because you are in your own home or in a private space that either you or the person you are speaking to controls, or are you in a public place or a government facility or some other facility that you don't control. As your Honor suggested, this courthouse, there are probably lots of security cameras all over the courthouse, and therefore, unless you are put in a room where someone from the court tells you, this is a private room where you can have a conversation with your client, I don't think that anyone can have a reasonable expectation of privacy outside of that location.

Again, same thing happens in all sorts of government facilities. It's true many of these cases have to do with police departments, because that is a more frequent occurrence. But the analogy to an embassy is very clear.

And your Honor, so for that reason, we believe there was no reasonable expectation of privacy with regard to those communications.

And just as a very small last point, about these IMEI numbers on the phones. It's true that -- I'm certainly not a cell phone expert, but it's true that these are numbers that

are written sort of on a phone, but they are not the electronic contents of the phone. But there are several cases, we cite a few of them, that say that by giving your phone to someone else, you have relinquished your expectation of privacy, including in this IMEI number that is inscribed on your phone, but is not part of the electronic contents of your phone.

THE COURT: I had taken the plaintiffs' argument to be that they're claiming protection for the inside of the phone, and they're referring to a card inside the phone.

MR. BARNEA: It is a physical card that is inserted into the phone. So it is inside physically, but it is not the electronic contents of the phone. So the Supreme Court's prohibition on requirement of a warrant is to what is on your phone. Your e-mails, your photographs, your files.

THE COURT: What is accessible from the inside of the phone?

MR. BARNEA: What is accessible electronically on the phone as opposed to the physical structure of the phone.

Serial numbers, little cards that are inside your phone that may be what help your phone access cell phone service and the like, those are not included within the Supreme Court's admonition.

THE COURT: So SIM cards.

MR. BARNEA: Precisely.

THE COURT: Are not.

1

2

3

4

5

6

7

8

9

10

11

12

13

14

15

16

17

18

19

20

MR. BARNEA: The information that you can see on the SIM card. If the government were to download the contents your SIM card, that would be different. But if the government were to simply open up the SIM card slot and take a picture of it and take down the SIM card number, that is not something that requires a warrant, if you've voluntarily provided that phone to the government or to somebody else. That's the distinction. THE COURT: What cases do you rely on for that?

MR. BARNEA: I thought you might ask that.

It is on page 17 of our opening brief. Ward v. Lee from the Eastern District of New York is a case that collects several cases about this.

THE COURT: Okay. Thank you.

MR. BARNEA: Thank you, your Honor.

THE COURT: I'll take the motion under advisement, and I look forward to the letter with the amendment and the response and the reply. Thank you, all.

MR. LEVENSON: Thank you, your Honor.

THE COURT: I appreciated the briefs and the argument.

(Adjourned)

21

22

23

24

25